



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,092	10/03/2003	David Andrew Thomas	200309084-1	3543

22879	7590	07/17/2007
HEWLETT PACKARD COMPANY		
P O BOX 272400, 3404 E. HARMONY ROAD		
INTELLECTUAL PROPERTY ADMINISTRATION		
FORT COLLINS, CO 80527-2400		

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/679,092	Applicant(s) THOMAS ET AL.	
	Examiner Benjamin E. Lanier	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 March 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 29 March 2007 amends claims 1, 8, 11, 12, 15, 27-30.

Applicant's amendment has been fully considered and entered.

Response to Arguments

2. Applicant's arguments with respect to claims 1-30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 21, 22, 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claim 21 provides for the use of a content server, one or more remote devices, a point of sale terminal, and a payment server, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced. Each element is described in the claims as being "operative" to perform certain functionalities, however, these specific functionalities are not positively recited in the claims such steps are required to be performed (see MPEP 2106 (II)).

Art Unit: 2132

6. Claim 22 includes multiple recitations of “a computer”, which renders the claim indefinite because it is unclear whether each recitation is intended to refer to separate computers or the same computer.

7. Claim 26 recites the limitation “the file server” in line 7. There is insufficient antecedent basis for this limitation in the claim.

8. Claim 26 recites, “code for receiving a confirmation of successful encrypted content download from the file server,” which renders the claims indefinite because the next claim limitation recites, “code for prompting the user to purchase the downloaded encrypted content.” It is unclear from the claims who downloaded the encrypted content, and from where the content was downloaded. It is believed that this indefiniteness stems from the “the file server” limitation mentioned above that lacks antecedent basis. Since it is unclear from the claims how “the file server” fits into the claim limitations, the limitation in question will be treated as the download of the encrypted content simply being confirmed.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 21, 30 are rejected under 35 U.S.C. 102(b) as being anticipated by Downs, U.S. Patent No. 6,226,618. Referring to claim 21, Downs discloses an electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a clearinghouse (Col. 19, steps 140-142), which meets the limitation of one or more remote

Art Unit: 2132

devices. Encrypted content is transmitted to the end-user device (Col. 19, step 148), which meets the limitation of a content server. An Electronic Digital Content Store handles content purchases for the end-users (Col. 18- Col. 19, steps 136-139), which meets the limitation of a point of sale terminal, and a payment server. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced. Each element is described in the claims as being “operative” to perform certain functionalities, however, these specific functionalities are not positively recited in the claims such steps are required to be performed (see MPEP 2106 (II)).

Referring to claim 30, Downs discloses an electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a clearinghouse (Col. 19, steps 140-142). The order SC includes the encrypted public key associated with the end-user device (Figure 1C & Col. 14, lines 47-61 & Col. 44, lines 9-12 & Col. 80, lines 26-27), which meets the limitation of means for receiving at least one identifier from a device, wherein the identifier is concealed and identifies the device. Encrypted content is transmitted to the end-user device (Col. 19, step 148), which meets the limitation of means for transmitted an encrypted file to the device. After verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of means for transmitting after receipt of an authorization, a decryption key encrypted using the identifier, wherein the decryption key can decrypt the encrypted file.

Claim Rejections - 35 USC § 103

Art Unit: 2132

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. Claims 18, 19, 24, 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, U.S. Patent No. 6,226,618. Referring to claim 18, Downs discloses an electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a clearinghouse (Col. 19, steps 140-142). The order SC includes the encrypted public key associated with the end-user device (Figure 1C & Col. 14, lines 47-61 & Col. 44, lines 9-12 & Col. 80, lines 26-27), which meets the limitation of sending a shared secret in an encoded form to a content server via an insecure communications channel because the clearinghouse can be included in the content store that hosts the content (Col. 10, lines 24-29 & Col. 11, lines 26-28). Encrypted content is transmitted to the end-user device (Col. 19, step 148), which meets the limitation of downloading from the content server an encrypted content via the insecure channel. Once received the end-user verifies the received content and transmits a result back to the content host (Col. 16, step 416). Downs does not specify that the result is encoded.

Art Unit: 2132

However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the result of Downs to be digitally signed prior to transmission so that the recipient of the result could verify the sender as taught by Downs (Col. 16, step 409). After verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of receiving a decryption key in an encrypted form from the content server via the insecure communications channel, wherein the decryption key is encrypted using the shared secret. Once received, the end-user decrypts the content key and uses the decrypted content key to decrypt the content (Col. 169, steps 417-418), which meets the limitation of decrypting the downloaded decryption key using the shared secret, decrypting the downloaded encrypted content using the decryption key. A result is sent by the end-user regarding the receipt of the content key (Col. 16, step 414), which meets the limitation of sending an acknowledgement of the received decryption key.

Referring to claim 19, Downs discloses that once the Electronic Digital Content Store receives credit card authorization for the purchase, the Content Store generates a transaction SC that is transmitted to the end-user to verify the transaction (Col. 19, steps 138-139). After verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of providing an indicia of acceptance of terms of the downloaded and decryption of the encrypted content by the user, wherein the indicia is an indication of acceptance of payment.

Referring to claim 24, Downs discloses an electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a clearinghouse (Col. 19, steps 140-142). The order SC includes the encrypted public key associated with the end-user device (Figure 1C & Col. 14, lines 47-61 & Col. 44, lines 9-12 & Col. 80, lines 26-27), which meets the limitation of code for sending a shared secret in an encoded form to a content server because the clearinghouse can be included in the content store that hosts the content (Col. 10, lines 24-29 & Col. 11, lines 26-28). Encrypted content is transmitted to the end-user device (Col. 19, step 148), which meets the limitation of code for receiving from the content server an encrypted content. Once received the end-user verifies the received content and transmits a result back to the content host (Col. 16, step 416). Downs does not specify that the result is encoded. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the result of Downs to be digitally signed prior to transmission so that the recipient of the result could verify the sender as taught by Downs (Col. 16, step 409). After verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of code for receiving an encrypted decryption key from the content server, wherein the decryption key is encrypted using the shared secret. The end-user decrypts the content key and then decrypts the content with the decrypted content key (Col. 16, steps 417-418), which meets the limitation of code for decrypting the encrypted decryption key using the shared secret, code for decrypting the downloaded encrypted content using the decryption key. The end-user verifies the content key upon receipt and transmits a result back to the sender (Col.

Art Unit: 2132

16, step 414), which meets the limitation of code for sending an acknowledgment of the received decryption key.

Referring to claim 25, Downs discloses that once the Electronic Digital Content Store receives credit card authorization for the purchase, the Content Store generates a transaction SC that is transmitted to the end-user to verify the transaction (Col. 19, steps 138-139). After verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of code for providing an indicia of acceptance of terms of the downloaded and decryption of the encrypted content by the user, wherein the indicia is an indication of acceptance of payment.

14. Claims 1-7, 20, 22, 23, 26-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, U.S. Patent No. 6,226,618, in view of vanHeyningen, U.S. Publication No. 2002/0112152. Referring to claim 1, Downs discloses an electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a clearinghouse (Col. 19, steps 140-142). The order SC includes the encrypted public key associated with the end-user device (Figure 1C & Col. 14, lines 47-61 & Col. 44, lines 9-12 & Col. 80, lines 26-27), which meets the limitation of providing, from a device via an insecure communications channel, at least one shared secret in encoded form that functions as an identifier of the device. Encrypted content is transmitted to the end-user device (Col. 19, step 148), which meets the limitation of transmitting encrypted content via the insecure communications channel from a content server to the device. After verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public

Art Unit: 2132

key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of receiving a confirmation authorizing release of a decryption key, and sending the decryption key to the device for decryption of the encrypted content. The process of purchasing content involves the end-user making selections of content they wish to purchase, followed by a purchase transaction process (Col. 18-Col. 19, steps 136-139) where the end-user public key is transmitted to the Electronic Digital Content Store (Col. 33, lines 35-37). Downs does not specify that this transaction process be performed using a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the content purchasing transactions between the end-user and the electronic digital content store of Downs to be conducted using a secure channel such as SSL because SSL provides a secure and convenient on-line shopping means for transmitting sensitive information, such as credit card numbers as taught by vanHeyningen ([0009]-[0010]).

Referring to claim 2, Downs discloses that once the Electronic Digital Content Store receives credit card authorization for the purchase, the Content Store generates a transaction SC that is transmitted to the end-user to verify the transaction (Col. 19, steps 138-139), which meets the limitation of wherein the confirmation is based on payment for the transmitted encrypted content.

Referring to claim 3, Downs discloses that the order SC includes the encrypted public key associated with the end-user device (Figure 1C & Col. 14, lines 47-61 & Col. 44, lines 9-12 & Col. 80, lines 26-27), which meets the limitation of the shared secret identifies a user, the device, or both.

Referring to claim 4, Downs discloses that the order SC also includes the encrypted credit card information (Col. 37, lines 18-24), which meets the limitation of the shared secret is a credit card number.

Referring to claim 5, Downs discloses that the end-user sends a result to the sender with respect to the receipt of the content key (Col. 16, step 414), which meets the limitation of receiving from the device an acknowledgement indicating receipt of the decryption key.

Referring to claim 6, Downs discloses that after verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of the decryption key is sent to the device via the insecure communication channel.

Referring to claim 7, Downs discloses that the clearinghouse receives the encrypted content key (Col. 19, step 141-142). Downs does not specify that this transaction process be performed using a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the between the end-user and the electronic digital content store/clearinghouse of Downs to be conducted using a secure channel such as SSL because SSL provides a secure and convenient on-line shopping means for transmitting sensitive information, such as credit card numbers as taught by vanHeyningen ([0009]-[0010]).

Referring to claim 20, Downs discloses an electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a clearinghouse (Col. 19, steps 140-142), which meets the limitation of prompting the user to accept terms of download and decryption of the encrypted content. The order SC includes the

Art Unit: 2132

encrypted public key associated with the end-user device (Figure 1C & Col. 14, lines 47-61 & Col. 44, lines 9-12 & Col. 80, lines 26-27), which meets the limitation of sending the shared secret to a content server because the clearinghouse can be included in the content store that hosts the content (Col. 10, lines 24-29 & Col. 11, lines 26-28). Encrypted content is transmitted to the end-user device (Col. 19, step 148), which meets the limitation of code for receiving from the content server an encrypted content. The received encrypted content includes a digest to verify the integrity of the content (Col. 16, step 416), which meets the limitation of receiving a confirmation of successful encrypted content download from the content server. After verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of after receipt of an indicia of such acceptance, sending an authorization to the content server to release a decryption key for decrypting the downloaded encrypted content.

Referring to claim 22, Downs discloses an electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a clearinghouse (Col. 19, steps 140-142). The order SC includes the encrypted public key associated with the end-user device (Figure 1C & Col. 14, lines 47-61 & Col. 44, lines 9-12 & Col. 80, lines 26-27), which meets the limitation of program code for causing a computer to receive a shared secret in an encoded form from a device, the encoded shared secret functioning as a device identifier. Encrypted content is transmitted to the end-user device (Col. 19, step 148), which meets the limitation of program code for causing a computer to transmit content in an encrypted form from a content server to the device. After verifying the authenticity of the order

Art Unit: 2132

SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of program code for causing a computer to receive a confirmation authorizing the release of a decryption key for the transmitted encrypted file, and program code for causing a computer to send the decryption key for decrypting the transmitted encrypted file for which the payment confirmation has been received. The process of purchasing content involves the end-user making selections of content they wish to purchase, followed by a purchase transaction process (Col. 18-Col. 19, steps 136-139) where the end-user public key is transmitted to the Electronic Digital Content Store (Col. 33, lines 35-37). Downs does not specify that this transaction process be performed using a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the content purchasing transactions between the end-user and the electronic digital content store of Downs to be conducted using a secure channel such as SSL because SSL provides a secure and convenient on-line shopping means for transmitting sensitive information, such as credit card numbers as taught by vanHeyningen ([0009]-[0010]).

Referring to claim 23, Downs discloses that once the Electronic Digital Content Store receives credit card authorization for the purchase, the Content Store generates a transaction SC that is transmitted to the end-user to verify the transaction (Col. 19, steps 138-139), which meets the limitation of wherein the confirmation is sent upon payment by a user of the device for the downloaded content.

Referring to claim 26, Downs discloses an electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a

Art Unit: 2132

clearinghouse (Col. 19, steps 140-142). The order SC includes the encrypted public key associated with the end-user device (Figure 1C & Col. 14, lines 47-61 & Col. 44, lines 9-12 & Col. 80, lines 26-27), which meets the limitation of code for sending the shared secret to a content server because the clearinghouse can be included in the content store that hosts the content (Col. 10, lines 24-29 & Col. 11, lines 26-28). Encrypted content is transmitted to the end-user device (Col. 19, step 148). The received encrypted content includes a digest to verify the integrity of the content (Col. 16, step 416), which meets the limitation of code for receiving a confirmation of successful encrypted content download from the file server. Downs discloses a pay per listen service (Col. 85, lines 55-59) that would allow a user to purchase the downloaded content each time they wish to listen to it, which meets the limitation of code for prompting the user to purchase the downloaded encrypted content. The process of purchasing content involves the end-user making selections of content they wish to purchase, followed by a purchase transaction process (Col. 18-Col. 19, steps 136-139) where the end-user public key is transmitted to the Electronic Digital Content Store (Col. 33, lines 35-37). Downs does not specify that this transaction process be performed using a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the content purchasing transactions between the end-user and the electronic digital content store of Downs to be conducted using a secure channel such as SSL because SSL provides a secure and convenient on-line shopping means for transmitting sensitive information, such as credit card numbers as taught by vanHeyningen ([0009]-[0010]).

Referring to claim 27, Downs discloses an electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a

Art Unit: 2132

clearinghouse (Col. 19, steps 140-142). The order SC includes the encrypted public key associated with the end-user device (Figure 1C & Col. 14, lines 47-61 & Col. 44, lines 9-12 & Col. 80, lines 26-27), which meets the limitation of receiving an identifier from a device as a concealed identifier identifies the device. Encrypted content is transmitted to the end-user device (Col. 19, step 148), which meets the limitation of transmitting an encrypted file to the device via an insecure channel, wherein the encrypted file has a corresponding decryption key. After verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of encrypting the key using the identifier, and transmitting the encrypted key to the device. The process of purchasing content involves the end-user making selections of content they wish to purchase, followed by a purchase transaction process (Col. 18-Col. 19, steps 136-139) where the end-user public key is transmitted to the Electronic Digital Content Store (Col. 33, lines 35-37). Once the Electronic Digital Content Store receives credit card authorization for the purchase, the Content Store generates a transaction SC that is transmitted to the end-user to verify the transaction (Col. 19, steps 138-139), which meets the limitation of receiving authorization from a payment server. Downs does not specify that this transaction process be performed using a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the content purchasing transactions between the end-user and the electronic digital content store of Downs to be conducted using a secure channel such as SSL because SSL provides a secure and convenient on-line shopping means for transmitting sensitive information, such as credit card numbers as taught by vanHeyningen ([0009]-[0010]).

Referring to claims 28, 29, Downs discloses an electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a clearinghouse (Col. 19, steps 140-142). The order SC includes the encrypted public key associated with the end-user device (Figure 1C & Col. 14, lines 47-61 & Col. 44, lines 9-12 & Col. 80, lines 26-27), which meets the limitation of means for receiving a shared secret/identifier in a concealed form, from a device, wherein the shared secret identifies the device. Encrypted content is transmitted to the end-user device (Col. 19, step 148), which meets the limitation of means for transferring a selected content in an encrypted form to the device wherein the selected file has a corresponding decryption key. After verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of means for using the shared secret/identifier to encrypt a decryption key, and means for transmitting the encrypted decryption key to a wireless device after receipt of payment. The process of purchasing content involves the end-user making selections of content they wish to purchase, followed by a purchase transaction process (Col. 18-Col. 19, steps 136-139) where the end-user public key is transmitted to the Electronic Digital Content Store (Col. 33, lines 35-37). Downs does not specify that this transaction process be performed using a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the content purchasing transactions between the end-user and the electronic digital content store of Downs to be conducted using a secure channel such as SSL because SSL provides a secure and convenient on-line shopping means for transmitting sensitive information, such as credit card numbers as taught by vanHeyningen ([0009]-[0010]).

15. Claims 8-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, U.S. Patent No. 6,226,618, in view of vanHeyningen, U.S. Publication No. 2002/0112152 as applied to claim 1 above, and further in view of Brickell, U.S. Patent No. 7,165,181. Referring to claims 8, 9, Downs does not disclose that the public key of the end-user is hashed with a random number. Brickell discloses a proof system wherein a public key is hashed along with a random number (Col. 6, lines 39-45), which meets the limitation of providing a random plaintext from the device, the shared secret is encoded by a hash function of a combination of the shared secret and the random plaintext. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the end-user in Downs to hash their public key with a random number in order to prove the identity of the end-user while maintaining privacy as taught by Brickell (Col. 1, lines 18-34 & Col. 7, lines 1-5).

Referring to claims 10, 11, Downs discloses that after verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of encrypting the decryption key before sending it to the device, the decryption key is encrypted using at least the shared secret.

Referring to claims 12, 14, 15, Downs disclose that the received encrypted content includes a digest to verify the integrity of the content (Col. 16, step 416). The end-user transmits a result of an integrity check for the received content back to the sender (Col. 16, lines 416). Downs does not disclose hashing the result with end-user public key and a random number. Brickell discloses a proof system wherein a public key is hashed along with a random number (Col. 6, lines 39-45), which meets the limitation of providing from the device a content

Art Unit: 2132

confirmation value that is encoded with the shared secret, the content download confirmation value is based on a calculation using the shared secret, providing a random plaintext from the device, providing a hash of the shared secret and the random plaintext for each shared secret, computing a hash of the shared secret with the random plaintext to produce a ciphertext for each shared secret. A second hash is used between the two devices in order to provide verification (Col. 6, lines 44-64), which meets the limitation of comparing the ciphertext to the hash of each of the shared secrets, and in the case of a match, identifying the corresponding transmitted encoded content, encoding a content download confirmation value for the transmitted encoded content using the shared secret, and comparing the computed content download confirmation value to the received content download confirmation value to verify a complete download. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the end-user in Downs to hash their public key with a random number in order to prove the identity of the end-user while maintaining privacy as taught by Brickell (Col. 1, lines 18-34 & Col. 7, lines 1-5).

Referring to claim 13, Downs discloses that the integrity result (Col. 16, step 415) is based on a hash which can be an MD5 hash (Col. 14, line 15), which meets the limitation of the content download confirmation value is based on an MD5 checksum.

Referring to claim 16, Downs discloses a pay per listen service (Col. 85, lines 55-59) that would allow a user to purchase the downloaded content each time they wish to listen to it. The electronic content delivery system wherein when an end-user selects content to purchase an order SC is built and transmitted to a clearinghouse (Col. 19, steps 140-142), which meets the limitation of after verification of the complete content download, causing a prompt to be sent to a

Art Unit: 2132

user of the device to purchase the downloaded content. Downs discloses that once the Electronic Digital Content Store receives credit card authorization for the purchase, the Content Store generates a transaction SC that is transmitted to the end-user to verify the transaction (Col. 19, steps 138-139). After verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device (Col. 44, lines 23-36 & line 56 – Col. 45, line 6), which meets the limitation of receiving a confirmation of receipt of payment.

Referring to claim 17, Downs discloses that encrypted content is transmitted to the end-user device (Col. 19, step 148), which meets the limitation of content stored in the content server is encrypted prior to a start of a download process.

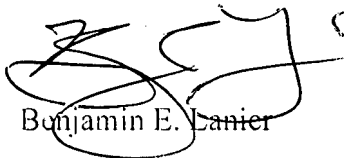
Conclusion

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier